UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

M.G., through his father and legal guardian BARTOSZ GRABOWSKI, individually and on behalf of all others similarly situated, Plaintiff, v. TIKTOK INC.; and BYTEDANCE, INC., Defendants.	MDL No. 2498 *This Document Relates to:* Case No.: 1:20-cv-05305 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

On behalf of himself and all others similarly situated, Plaintiff M.G., a minor, by and through his father and legal guardian Bartosz Grabowski (collectively, "Plaintiff"), brings this Class Action Complaint against Defendants TikTok Inc. ("TikTok") and ByteDance, Inc. ("ByteDance"). Plaintiff seeks damages to redress Defendants' unlawful collection, storage, use, and disclosure of biometric identifiers[1] and biometric information[2] (collectively, "biometrics") in clear violation of the Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*,; restitution for Defendants' profiting from the same; and equitable relief to prevent further disclosure of his biometrics as part of ByteDance's upcoming divestment of TikTok's assets to a soon-to-be-revealed entity (hereinafter, the "Acquiring Entity"). Plaintiff demands a trial by jury, and alleges as follows based on personal knowledge as to himself, on the investigation of his counsel, and on information and belief as to other matters.

NATURE OF ACTION

1. In March 2008, Pay By Touch, then the largest operator of fingerprint-based payment-verification services in Illinois, declared bankruptcy. *See* 95th Ill. Gen. Assem., House Proceedings, May 30, 2008, at 249 (statement of Rep. Ryg). As a result of that declaration,

[1] A "biometric identifier" is a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.

[2] "Biometric information" is any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.

"thousands of customers from Albertson's, Cub Foods, Farm Fresh, Jewel Osco, Shell, and Sunflower Market" were left "wondering what [would] become of their biometric and financial data." *Id.* They didn't wonder for long, though; the bankruptcy court quickly thereafter approved a sale of Pay By Touch's biometric-payment database.

2. Immediately thereafter, in May 2008, the Illinois Legislature recognized the importance of protecting individuals' biometric privacy, finding that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

3. To ensure the security of individuals' biometrics, the Illinois Legislature enacted BIPA, which provides, *inter alia*, a private entity may not possess an individual's biometrics unless it: (1) informs them in writing that biometric identifiers or information will be collected or stored; (2) informs them in writing of the specific purpose and duration for which such biometric identifiers or biometric information is being collected, stored, and used; (3) receives a written release for the collection of their biometric identifiers or information; and (4) publishes publicly available written retention schedules and guidelines for permanently destroying biometric identifiers and biometric information, 740 ILCS 14/15.

4. TikTok owns and operates a popular mobile application (the "TikTok App") that is used by over 100 million people in the United States to create and share short music videos in a social network-like environment. Children comprise the majority of the TikTok App's userbase.

5. The TikTok App makes various audio and visual features and effects available for its users to apply to their videos—including lip-syncing tools, face filters, face trackers (which automatically zoom in on a user's face when the camera lens detects it), and voice-alteration filters.

6. However, Defendants use those features to collect, store and use the "face templates" (or "scans of face geometry") and "voiceprints" of their users. Defendants do this

without notifying their users or making available any policies governing use or destruction of this immutable data, much less obtaining users' consent. Each voiceprint and face template that Defendants extract and catalogue in their vast Orwellian biometrics database is personally unique, in the same way that a fingerprint uniquely identifies one and only one person.

7. Defendants use the "biometric identifiers" that they have collected to derive other personally identifying "biometric information" pertaining to their users, including age, gender, race, and emotional state, all of which is then linked with the user's name, e-mail address, and other unique identifiers in their database. Thus, in direct violation of BIPA, Defendants collect, store, and use millions of Illinoisans' biometrics—including millions of children's—without obtaining the requisite release or publishing the mandated data-retention policies.

8. Defendants amassed this trove of immutable biometric data to train and further develop their invasive technology, grow their business, and make money. In fact, in October 2018, shortly after it had unleashed the TikTok App on the world's consuming public, ByteDance boasted that "[t]he large userbase of our platforms has ensured a continuous influx of valuable user data that we are using to refine our existing models and think of new applications to improve user experience. This virtuous cycle of AI has allowed us to venture into areas of machine intelligence the world has not seen before."[3]

9. On August 6 and 14, 2020, the President of the United States issued two executive orders compelling ByteDance to divest TikTok's assets to a domestic entity by no later than September 20, 2020 or cease doing business in the United States, and ordering Defendants to divest all data pertaining American users no later than November 12, 2020. In the course of its ongoing—and highly public—sales efforts, TikTok maintains that it will transfer its users' data (including their biometrics) to any acquiring entity. TikTok cannot be allowed to sell its users' biometric

[3] Internet Archive: Wayback Machine, "Home Page – ByteDance AI Lab," cached version of http://ailab.bytedance.com/ dated Oct. 17, 2018 and published by ByteDance Inc. AI Lab, *available at* https://web.archive.org/web/20181017170408/http://ailab.bytedance.com/ (last accessed Sept. 8, 2020).

data to the highest bidder; that is the precise scenario that triggered BIPA's passage in the first place.

10. Plaintiff and the other Illinoisans who have had their biometric data surreptitiously collected and stored by Defendants are entitled by law to have this sensitive data permanently destroyed. Further dissemination of their biometrics would deny BIPA's promise of privacy precisely where it is needed the most. Thus, to ensure that Defendants destroy, rather than disclose, Plaintiff's and the Class's purloined biometric data, Plaintiff seeks not only the damages available by law, but also restitution, and an injunction barring Defendants from transferring their biometric data to any other entity.

JURISDICTION AND VENUE

11. The Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000 and because Defendants are each citizens of a state different from that of at least one class member.

12. This Court has personal jurisdiction over Defendants because they collected Plaintiff's biometrics within Illinois; Defendants failed to provide the requisite notice or obtain the requisite written release from Plaintiff in Illinois; and because Defendants use content-delivery network (CDN) and edge servers in Illinois that collect, transmit, use, and store Plaintiff's biometrics.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Plaintiff resides in Cook County, which is within this District; because Plaintiff had his biometrics unlawfully collected from within this District; because Defendants use content-delivery network (CDN) and edge servers in this District that collect, transmit, use, and store Plaintiff's biometrics; because Defendants failed to provide the notices or obtain the releases necessary from their users in this District; and because Plaintiff suffered his injuries within this District.

PARTIES

14. Plaintiff M.G. and his father and natural legal guardian Bartosz Grabowski are, and at all relevant times have been, citizens of the State of Illinois residing in Mt. Prospect, Illinois, which is within Cook County.

15. Defendant TikTok Inc. f/k/a Musical.ly, Inc. ("TikTok") is a California corporation with its principal place of business in Culver City, California. Defendant TikTok maintains offices and conducts business in Chicago, Illinois.

16. Defendant ByteDance, Inc. is a Delaware corporation with its principal place of business in Palo Alto, California. ByteDance, Inc. maintains offices and conducts business in Chicago, Illinois.

FACTUAL BACKGROUND

I. BIOMETRIC PRIVACY CONCERNS TRIGGER BIPA'S ENACTMENT

A. Biometric Technology Implicates Consumer Privacy Concerns

17. "Biometrics" refers to unique physical characteristics used to identify an individual. One of the most prevalent uses of biometrics is in facial recognition technology, which works by scanning a human face or an image thereof, extracting facial feature data based on specific "biometric identifiers" (*i.e.*, details about the face's geometry as determined by facial points and contours), and comparing the resulting "face template" (or "faceprint") against the face templates stored in a database. If a match is found, an individual can be identified.

18. The use of facial-recognition technology in the commercial context presents numerous consumer privacy concerns. During a 2012 hearing before the United States Senate Subcommittee on Privacy, Technology, and the Law, Senator Franken—then the Chairman of the Subcommittee—stated that "there is nothing inherently right or wrong with facial recognition technology … But if we do not stop and carefully consider the way we use this technology, it may also be abused in ways that could threaten basic aspects of our privacy and civil liberties."[4] Senator

[4] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1

Franken noted, for example, that facial recognition technology could be "abused to not only identify protesters at political events and rallies, but to target them for selective jailing and prosecution."[5]

19. The Federal Trade Commission ("FTC") has raised similar concerns, and recently released a "Best Practices" guide for companies using facial recognition technology.[6] In the guide, the Commission underscores the importance of companies' obtaining affirmative consent from consumers before extracting and collecting their biometric identifiers and biometric information from digital photographs.

20. Voiceprinting is another prominent form of biometrics. "Voiceprint refers to the acoustic frequency spectrum that carries the speech information in a human voice. Like fingerprints, it has unique biometric signatures, is individual-specific, and can function as an identification method."[7]

21. Like faceprinting, however, voiceprinting carries substantial privacy and security risks. Given the ubiquitous presence of internet-enabled and microphone-connected devices in modern life, voiceprinting technology embedded in a common software package (like the TikTok App) would allow for precise tracking of an individual over time based on where their voice appeared. Moreover, were an individual's voiceprint to be compromised or disclosed, it would

(2012), *available at* https://www.judiciary.senate.gov/imo/media/doc/12-7-8FrankenStatement.pdf (emphasis in original) (last accessed Sept. 8, 2020).

[5] *Id.*

[6] *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade Commission (Oct. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf (last accessed Sept. 8, 2020).

[7] *Voiceprint Recognition – Not Just a Powerful Authentication Tool*, Alibaba Cloud (Mar. 17, 2017), https://www.alibabacloud.com/blog/voiceprint-recognition-system-e28093-not-just-a-powerful-authentication-tool_72408.

create a substantial risk of identity theft and other misconduct. In effect, a bad actor possessing an individual's voiceprint could use it to fabricate speech by that individual.[8]

B. The Illinois Biometric Information Privacy Act

22. In 2008, Illinois enacted the BIPA due to the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276. The BIPA makes it unlawful for a company to*, inter alia*, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers[9] or biometric information, unless it first:

> (l) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative."

740 ILCS 14/15 (b).

23. Section 15(a) of the BIPA also provides:

> A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 ILCS 14/15(a).

[8] ByteDance itself has boasted of similar technology, with the head of its AI lab showing how its technology could allow for real-time translation of an individual's speech into another language, using the speaker's own voice. *See [4/24 Live] Keynote Speech by Wei-Ying Ma | WWW 2020*, YouTube (Apr. 23, 2020), https://youtu.be/2D29f4-J2mw?t=2400.

[9] BIPA's definition of "biometric identifier" expressly includes information collected about the geometry of the face (i.e., facial data obtained through facial recognition technology), and "voiceprint." *See* 740 ILCS 14/10.

24. As alleged below, Defendants violated all three prongs of § 15(b) of BIPA by collecting, storing, and using biometric identifiers and biometric information from persons in Illinois, including millions of children, without first obtaining the requisite informed written consent. Defendants' failure to provide a publicly available written policy regarding its schedule and guidelines for the retention and permanent destruction of this biometric data also violates BIPA § 15(a).

II. THE RISE OF BYTEDANCE AND TIKTOK

A. ByteDance Becomes one of the Most Powerful Tech Companies in the World

25. ByteDance Ltd. was founded in 2012 by Zhang Yiming on the principle that artificial intelligence (AI) would accelerate the transition to the smartphone as the world's predominant consumer-information interface. "ByteDance regards its platforms as part of an artificial intelligence company powered by algorithms that 'learn' each user's interests and preferences through repeat interaction."[10]

26. To that end, in its first few years, ByteDance released a number of smartphone apps utilizing its AI technologies. When those apps became nearly ubiquitous in the Chinese market, ByteDance's AI platform only improved further, setting up a recursive process whereby growth fueled AI improvements, which in turn fueled further growth.

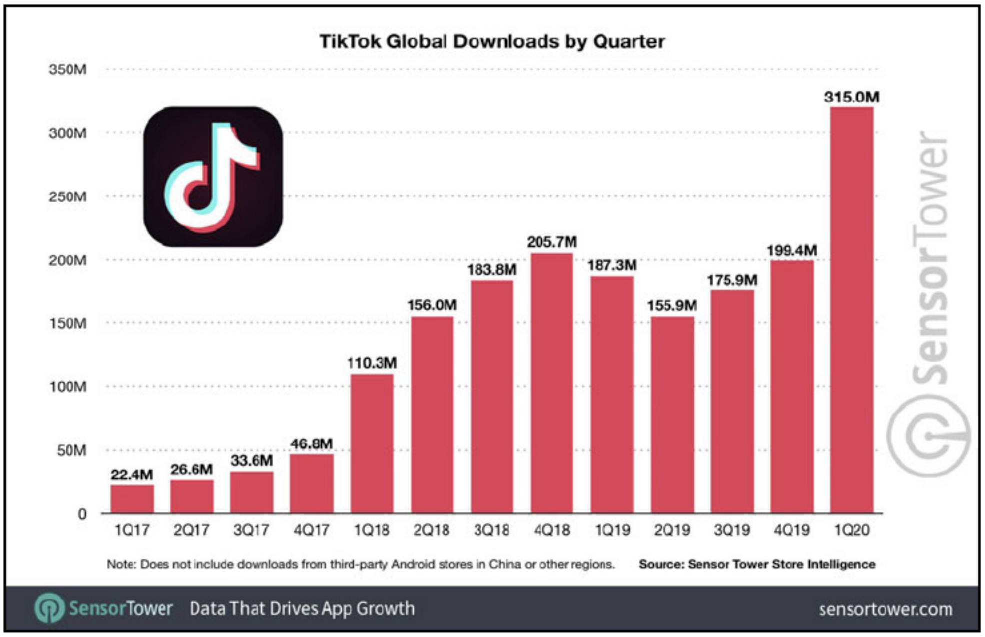
27. In 2016 and 2017, ByteDance launched Douyin and TikTok, respectively. The apps were substantively identical (with Douyin serving the Chinese market, and TikTok serving Japan, Thailand, Vietnam, Indonesia, India, and Germany), and imitated the popular app Musical.ly, by allowing users to create short dance, lip-sync, comedy, and talent videos. Leveraging its advanced AI to create a highly addictive user experience, Douyin grew to have 400 million active daily users by January 2020. Douyin and TikTok, however, had no presence in the United States.

[10] Letter from Sens. Tom Cotton and Chuck Schumer, to Joseph McGuire, Acting Director of National Intelligence, (Oct. 25, 2019), *available at* https://www.democrats.senate.gov/imo/media/doc/10232019%20TikTok%20Letter%20-%20FINAL%20PDF.pdf.

B. ByteDance Acquires Musical.ly and Transforms it Into TikTok, Which Quickly Becomes one of the Most Downloaded Apps of All Time

28. ByteDance entered the U.S. market in 2017 with its acquisition of Musical.ly, worth up to $1 billion at the time.[11] In August 2018, ByteDance formally merged Musical.ly into TikTok and thereafter transferred all of Musical.ly's user accounts and data to TikTok.[12]

29. By combining Musical.ly's lip-syncing platform with ByteDance's advanced data mining and analytics technologies, the TikTok App quickly evolved into one of the most popular mobile apps among American consumers, gaining over 680 million active monthly users by the end of 2018[13] and surpassing two billion downloads in April 2020, as reflected in the chart below:[14]


TikTok Global Downloads by Quarter

Note: Does not include downloads from third-party Android stores in China or other regions. Source: Sensor Tower Store Intelligence

[11] Rishi Iyengar, *In sync: China's hottest news app buys Musical.ly*, CNN Business (Nov. 10, 2017), https://money.cnn.com/2017/11/10/technology/musically-bytedance-toutiao-china/index.html.

[12] Alex Weprin, *Musical.ly To Shut Down*, MediaPost (Aug. 2, 2018), https://www.mediapost.com/publications/article/323111/musically-to-shutdown.html.

[13] *TikTok Statistics – Updated August 2020*, Wallroom Media (Aug. 25, 2020), https://wallaroomedia.com/blog/social-media/tiktokstatistics/.

[14] Manish Singh, *TikTok tops 2 billion downloads*, TechCrunch (Apr. 29, 2020), https://techcrunch.com/2020/04/29/tiktok-tops-2-billiondownloads/.

30. Not only has the TikTok App's popularity led to countless celebrities joining the platform – such as, for example, Will Smith, Britney Spears, Alex Rodriguez, and Jennifer Lopez, each of whom has millions of followers[15] – many of its young users have become celebrities in their own right by creating and sharing viral videos and other content on the TikTok App.[16]

31. It thus comes as little surprise that children make up a substantial portion of the TikTok App's user demographic. In September 2016, the *New York Times* described Musical.ly as "an app that is young in every sense of the word," noting that the company claimed to have over 100 million users, mostly between ages 13 and 20; the *Times* observed: "What is striking about the app, though, is how many of its users appear to be even younger than that."[17] In February 2020, *The Wall Street Journal* reported that TikTok's "youthful vibe presents a predicament for TikTok because many devotees are under 13."[18] In particular, the article reported that approximately 70% of 10-year-old girls with smartphones in the U.S. downloaded and used the TikTok App in 2019.[19] Moreover, the average 10-year-old girl using the TikTok App spends more than four hours a week on the app, equivalent to more than 1,000 videos.[20]

32. Defendants have historically monetized their large user base through at least two avenues: in-app purchases of "coins" and traditional online advertising. TikTok App users are able

[15] Dusty Baxter-Wright, *The best celebrities to follow on TikTok*, Cosmopolitan (Apr. 3, 2020), https://www.cosmopolitan.com/uk/entertainment/a32028959/celebrities-on-tik-tok/.

[16] Paige Leskin, *Charli D'Amelio has taken over as TikTok's biggest star. These are the 40 most popular creators on the viral video app*, Business Insider (Mar. 25, 2020), https://www.businessinsider.com/tiktok-most-popular-stars-gen-z-influencers-social-media-app-2019-6.

[17] John Herrman, *Who's Too Young for an App? Musical.ly Tests the Limits*, N.Y. Times (Sept. 16, 2016), https://www.nytimes.com/2016/09/17/business/media/a-social-network-frequented-by-children-tests-the-limits-of-online-regulation.html.

[18] Georgia Wells and Yoree Koh*, TikTok Wants to Grow Up, but Finds It Tough to Keep Kids Out*, Wall Street Journal (Feb. 16, 2020), https://www.wsj.com/articles/tiktok-wants-to-grow-up-but-finds-it-tough-to-keep-kids-out-11581858006.

[19] *Id.*

[20] *Id.*

to purchase "coins," a virtual currency, to "reward" other users for creating entertaining videos.[21] Content creators are then able to cash out these coins for real money.

33. Defendants generate substantial revenue by selling advertising space on the TikTok App, primarily in the form of video ads that appear in between user-generated content.[22]

34. Whenever a user clicks on one of these ads and/or purchases the advertised product, Defendants are paid a fee by the advertiser. Defendants generated over $50 million in revenue in the fourth quarter of 2019 alone, attributable to a 310% rise in in-app purchase revenue from the prior year.[23]

C. Defendants Collect Troves of Personally Identifying and Uniquely Identifying Device Data from Both Prospective and Enrolled TikTok Users

35. To generate content and interact with other users on the TikTok App, an individual must create an account by submitting their telephone number, email address, or Facebook account information (which in turn provides these personal details and more to TikTok).[24]

36. After a new account is opened, the TikTok App searches the user's phone contacts and social-media followers to identify acquaintances already enrolled with TikTok, and then allows the user to search for videos by a particular category (e.g., sports), perform advanced searches by hashtag or a particular user, comment on videos and directly message other users, and create and submit their own video content.

[21] Sean Keach, *PAY PER VIEW How TikTok tempts kids to spend hundreds of pounds on virtual coins to pay 'online celebs'*, The U.S. Sun (Mar. 1, 2020), https://www.the-sun.com/lifestyle/tech/475150/how-tiktok-tempts-kids-to-spend-hundreds-of-poundson-virtual-coins-to-pay-online-celebs/.

[22] Tom Beat, *How Does TikTok Make Money? Overview of the Business Model*, InfoBeat, https://infobeat.com/how-does-tiktok-make-money-overview-of-the-business-model (last accessed Sept. 8, 2020).

[23] Alex Wilhelm, *TikTok's revenue said to skyrocket over 300% in Q4*, TechCrunch (Jan. 3, 2020), https://techcrunch.com/2020/01/03/tiktoks-revenue-said-to-skyrocket-over-300-in-q4/

[24] Frannie Ucciferri, *Parents' Ultimate Guide to TikTok*, Common Sense Media (July 22, 2020), https://www.commonsensemedia.org/blog/parents-ultimate-guide-to-tiktok.

37. The amount of data siphoned from users and their devices is comprehensive, including the user's name, age, e-mail address, telephone number, social media account information, payment method data, contact list,[25] all user-generated content (e.g., videos and photographs recorded on its app), communication history, IP addresses, geo-location-related data, device identifiers, browsing and search history (both on and off the TikTok app), cookies, and metadata, among other sensitive data.[26]

38. In addition to harvesting data directly from its users, Defendants scour third parties for data about its users, including social networks such as Facebook, advertising companies, data miners, data brokers, data appenders, and other TikTok users.[27]

39. After collecting all of this highly sensitive data pertaining to a user, Defendants then "process[], . . . scan and analyze" the information,[28] and "may share [it] with a parent, subsidiary, or other affiliate of [its] corporate group."[29]

40. Although Defendants maintain a separate privacy policy for children, referred to as its "Privacy Policy for Younger Users,"[30] this policy reveals that they *still* systematically collect, catalog, and analyze their personal information, including users' birthdays, and "certain information automatically from the user's device, including internet or other network activity information such as device ID, IP address, web browser type and version, country-level location,

[25] *Privacy Policy*, TikTok (last updated Jan. 1, 2020), https://www.tiktok.com/legal/privacy-policy?lang=en#privacy-us; Echo Wang, Alexandra Alpher, Yingzhi Yang, *Exclusive: China's ByteDance moves to ringfence its TikTok app amid U.S. probe – sources*, Reuters (Nov. 27, 2019), https://www.reuters.com/article/usbytedance-tiktok-exclusive/exclusive-chinas-bytedance-moves-to-ringfence-its-tiktok-app-amid-us-probesources-idUSKBN1Y10OH.

[26] *Privacy Policy*, *supra* note 25.

[27] *Id.*

[28] *Id.*

[29] *Id.* In prior versions of the Privacy Policy, TikTok specifically states that it "will" share user information with "any member or affiliate of our group, in China[.]" *See, e.g.*, , Internet Archive: Wayback Machine, "Privacy Policy," cached version of http:/www.tiktok.com/i18n/privacy #how-share dated August 2018 and published by TikTok, *available at* https://web.archive. org/web/20180829183230/http:/www.tiktok.com/i18n/privacy#how-share.

[30] *Available at Privacy Policy for Younger Users*, TikTok (last updated January 2020), https://www.tiktok.com/legal/privacy-policy-for-younger-users?lang=en.

as well as certain app activity data, such as video watches, time in the app, and general usage data."[31] Notably, the TikTok App permits children to create TikTok accounts and use the TikTok App without any receiving confirmation that the children or their parents or guardians have even seen or reviewed the TikTok App's privacy policies or terms of service.

D. Defendants Fail to Adequately Protect the Data they Collect from their Users, Including their Child Users

41. As if Defendants' practices of surreptitiously amassing the personal and biometric data of children were not offensive enough, Defendants have also failed to maintain this sensitive data in confidence or safeguard the vast database that houses it.

42. One expert in the field of data protection, Matthias Eberl, performed "a detailed privacy check of the TikTok app and its corresponding website," and found multiple transparency and data protection concerns, including evidence of TikTok's use of invasive digital fingerprinting technology and its transmission of device information, usage time, video viewing history, and user search terms to third parties (including Facebook).[32]

43. On October 23, 2019, Senators Tom Cotton (R-Arkansas) and Chuck Schumer (D-New York) sent a letter to Acting Director of National Intelligence Joseph Maguire, requesting a formal assessment of the particular national security risks posed by TikTok in light of Chinese cybersecurity laws mandating Chinese companies' cooperation with the Chinese government's intelligence work.

44. In November 2019, it was reported that the Committee on Foreign Investment in the United States ("CFIUS") had initiated an inquiry concerning TikTok's stewardship of U.S.-based users' personal data and any transmissions of such data to China.[33]

[31] *Id.*

[32] Matthis Eberl, *Privacy Analysis of Tiktok's App and Website*, Rufposten (Dec. 5, 2019).

[33] Wang, Alper, and Yang, s*upra* note 25; Jack Nicas, Mike Isaac, and Ana Swanson, *TikTok Said to Be Under National Security Review*, N.Y. Times (Updated Aug. 7, 2020), https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html.

45. Subsequently, an analysis of the TikTok App performed by Penetrum Security found that TikTok App users' personal data was indeed being cataloged on servers in China, stating: "From our understanding and our analysis, it seems that TikTok does an excessive amount of tracking on its users and that the data collected is partially if not fully stored on Chinese servers with the ISP Alibaba."[34]

46. Alibaba, interestingly enough, suffered a data breach that included "IMEI, IMSI, phone numbers, and user data specifically pertaining to phones was breached as well as other personal information."[35] In other words, not only were Defendants storing user data in China, "the data collected" by them "is mentioned in a breach that happened to their ISP provider" in China.[36]

47. In January 2020, a report issued by Checkpoint Research noted that it had "discovered multiple vulnerabilities within the TikTok application," which "allow attackers to … [g]et a hold of TikTok accounts and manipulate their content, "[d]elete videos," "[u]pload unauthorized videos," "[m]ake private 'hidden' videos public," and "[r]eveal personal information saved on the account such as private email addresses."[37]

48. By the end of January, each branch of the U.S. military had grown so concerned about Defendants' data-safety record that they banned the use of the TikTok App on all government-owned mobile devices.[38]

49. And the following month, Reddit's Chief Executive Officer Steve Huffman called TikTok "fundamentally parasitic," because "it's always listening, the fingerprinting technology

[34] Penetrum Security, "Penetrum Security Analysis of TikTok versions 10.0.8 - 15.2.3" at p.11, *available at* https://penetrum.com/tiktok/Penetrum_TikTok_Security_Analysis_whitepaper.pdf

[35] *Id.*

[36] *Id.*

[37] Alon Boxiner, et al., *Tik or Tok? Is TikTok secure enough?*, Check Point Research (Jan. 8, 2020), https://research.checkpoint.com/2020/tik-or-tok-is-tiktok-secure-enough/.

[38] Kalhan Rosenblatt, *Army bans TikTok following guidance from the Pentagon*, NBC News (Dec. 31, 2019), https://www.nbcnews.com/tech/tech-news/u-s-army-bans-tiktok-following-guidance-pentagonn1109001.

that they use is truly terrifying, and I could not bring myself to install an app like that on my phone."[39]

50. On March 12, 2020, the "No TikTok on Government Devices Act" was introduced in the U.S. Senate. The bill would ban all federal employees from using TikTok on any device issued by the United States or a government corporation in an effort to address what the bill's sponsors perceived as a national-security threat posed by TikTok's data collection.[40]

51. Other countries have echoed the United States' concerns about TikTok's data-privacy practices. For instance, on May 8, 2020, the Dutch Data Protection Authority announced that it had begun investigating whether TikTok was adequately protecting the data it collects from children under Dutch law and the European Union's General Data Protection Regulation.[41]

52. U.S. consumers have also taken TikTok to task for its improper collection and usurpation of users' personal data. For example, in October 2018, one TikTok App user voiced concern after discovering that TikTok had taken still photos from the "private" videos he had recorded and used them for its own advertising purposes on Facebook.[42] The individual learned of TikTok's nonconsensual use of his videos in this manner from third parties who had informed him that his face appeared in advertisements for the TikTok App on Facebook.

III. DEFENDANTS VIOLATE BIPA ON AN UNPRECEDENTED SCALE

53. In addition to collecting a trove of private and uniquely identifying personal and device-related data about every user of the TikTok App, most of whom are children, Defendants have also developed and unleashed sophisticated and immensely powerful biometrics-collection

[39] Lucas Matney, *Reddit CEO: TikTok is 'fundamentally parasitic'*, TechCrunch (Feb. 26, 2020), https://techcrunch.com/2020/02/26/reddit-ceo-tiktok-is-fundamentally-parasitic/.

[40] *Senators Hawley, Scott Introduce Legislation to Ban TikTok from Government Devices*, Josh Hawley: U.S. Senator for Missouri (Mar. 12, 2020), https://www.hawley.senate.gov/senators-hawley-scott-introduce-legislation-ban-tiktok-governmentdevices.

[41] *Dutch Data Protection Authority to investigate TikTok*, Autoriteit Persoonsgegevens (May 8, 2020), https://autoriteitpersoonsgegevens.nl/en/news/dutch-data-protection-authority-investigate-tiktok.

[42] Cody Ko, *Tik Tok is trolling me*, YouTube (Oct. 30, 2018), https://www.youtube.com/watch?v=SDdR8cue4eE.

technology on its users, including children. This technology extracts and analyzes the acoustic details and characteristics of the human voices and the detailed geometric patterns and measurements of the human faces (including the contours of faces and the distances between certain localized facial points, such as the distances between eyes and noses and ears) that appear in every each and video uploaded by each and every user of the TikTok App worldwide.

54. Specifically, whenever a voice appears in a video uploaded by a user (including a child user) of the TikTok App, Defendants extract, collect, store, and catalog the speaker's "voiceprint"—a unique, immutable, and highly sensitive biometric identifier used to identify a person—in their vast database of personally identifying biometric voice data.

55. Likewise, whenever a face appears in a video uploaded by a user (including a child user) of its TikTok App, Defendants extract, collect, store, and catalog a "scan of face geometry" (also known as a "face template") pertaining to the person's face—another unique, immutable, and highly sensitive biometric identifier used to identify a person—in their vast database of personally identifying biometric facial data.

56. Accordingly, Defendants have collected the "biometric identifiers" of every person, including every child, whose voice or face appears in a video uploaded via its TikTok App in Illinois and elsewhere across the world, including the "biometric identifiers" of Plaintiff and numerous other persons in Illinois (among them millions of children). *See* 740 ILCS 14/10.

57. Defendants do more than just use biometrics to identify their users (mostly children) by name; they also use biometrics to identify users' gender, age, race, and emotional state.[43] Accordingly, Defendants collect the "biometric information" of every person whose voice or face appears in a video uploaded via the TikTok App in Illinois (or anywhere else the world). *See* 740 ILCS 14/10.

[43] *See Effect sdk 2.0*, ByteDance, Inc., *available at* http://ailab.tobsnssdk.com/ (last accessed Sept. 8, 2020).

58. Plaintiff is informed and believes that, during the period of time relevant to this action, TikTok has stored its users' data, including biometric data, at various "edge network" (or "content delivery network") data centers throughout the country operated by Fastly, Inc. and Akamai, Inc.[44]

59. The data of Plaintiff and the other members of the proposed Class, all of whom reside in Illinois, is stored by TikTok at Akamai's and Fastly's data centers in Chicago, Illinois.[45]

60. At no time have did Defendants notify Plaintiff or any members of the Illinois Voice Subclass or Illinois Face Subclass (or any of their parents in the case of minors) of the specific purpose and length of term for which their (or their children's) biometric identifiers and information would be collected, stored, and used, nor did Defendants obtain written releases from Plaintiff or any members of the Illinois Voice Subclass or Illinois Face Subclass (or any of their parents). Thus, Defendants collected, stored, and used, from within Illinois, Plaintiff's and the Illinois Voice Subclass and Illinois Face Subclass members' biometrics in direct violation of §§ 15(b)(2) and 15(b)(3) of BIPA.

[44] *See* Kevin Cook Zacks, *Bull of the Day: Fastly*, Yahoo! Finance (June 15, 2020), https://finance.yahoo.com/news/bull-day-fastly-fsly-090609924.html ("Fastly is classified as a Content Delivery Network (CDN) like Akamai (AKAM) and they both serve the fast growing social media platform TikTok[.]"); *Fastly, Inc. Form 10-Q for the Quarterly Period Ending June 30, 2020*, U.S. Securities and Exchange Commission, Aug. 7, 2020, *available at* https://d18rn0p25nwr6d.cloudfront.net/CIK-0001517413%20/7d22d29d-7c13-4fe6-9582-b691ee27de79.pdf (last accessed Sept. 8, 2020) ("ByteDance, the operator of the TikTok application, operates in and has strong business ties to China and is our top customer, accounting for 13% and 12% of revenue for the three and six months ended June 30, 2020, respectively.").

[45] *See Status*, Fastly, Inc., *available at* https://status.fastly.com/ (last accessed Sept. 8, 2020) (identifying four edge data centers operated by Fastly in Chicago, IL); *Media Delivery Network Map*, Akamai, Inc., *available at* https://www.akamai.com/us/en/resources/visualizing-akamai/media-delivery-map.jsp (last accessed Sept. 8, 2020) (identifying Akamai storage network and media network location in Chicago, IL); *List of Cloud Data Centers Accessible Via Akamai's Private Network Connectivity*, Akamai, Inc., *available at* https://www.akamai.com/us/en/what-we-do/cloud-service-providers.jsp#azure-list (last accessed Sept. 8, 2020) (identifying Akamai "North Central US" cloud data center in Illinois).

61. In direct violation of § 15(a) of the BIPA, Defendants do not have written, publicly available policies identifying their retention schedules, or guidelines for permanently destroying the biometric identifiers and biometric information that they have collected from Illinoisans and stored in their database.

62. Defendants use the voiceprints and face templates they collect to, *inter alia*, identify and track the individual users (including children) whose faces and voices appear in videos that are uploaded via the TikTok App, further enhancing the capabilities of their App's features and the formidability of their brand.

63. For instance, it has been revealed that Douyin – Defendants' Chinese market version of TikTok – contains a feature, powered by Defendants' facial recognition technology, that allows users to select an individual's face in a video and identify other videos (uploaded by other users) in which that person appears.[46] This technology works by comparing the face templates collected from the faces (or the voiceprints collected from the voices in the case of Defendants' voice recognition technology) that appear in newly uploaded videos with the face templates (or voiceprints) already saved in Defendants' vast biometrics database, collected both from the "identity verification" process that users go through at the time of enrollment and from the biometrics extracted from previously uploaded videos.

64. Defendants use of facial-recognition technology is not limited to Douyin, however. In January 2020, Israeli market-research startup Watchful.ai discovered code in the Douyin and TikTok Android apps that would allow users to create "deepfake" videos of themselves. "Deepfakes refer to manipulated videos, or other digital representations produced by sophisticated artificial intelligence that yield fabricated images and sounds that appear to be real."[47]

[46] Adan Korhnhorst, *TikTok's New "Video Search" Function is From the Future*, Radii (Sept. 26, 2019), https://radiichina.com/tiktok-new-video-search-function-is-from-the-future/.

[47] Grace Shao, *What 'deepfakes' are and how they may be dangerous*, CNBC (Oct. 13, 2019), https://www.cnbc.com/2019/10/14/what-is-deepfake-and-how-it-might-be-dangerous.html.

65. While Defendants' deepfake maker was not yet activated to the public, the underlying technologies were all present in the app. When Watchful.ai activated the code, the deepfake process worked as follows: "First, users scan their face into TikTok. This also serves as an identity check to make sure you're only submitting your own face so you can't make unconsented deepfakes of anyone else using an existing photo or a single shot of their face. By asking you to blink, nod and open and close your mouth while in focus and proper lighting, Douyin can ensure you're a live human and create a manipulable scan of your face that it can stretch and move to express different emotions or fill different scenes."[48]

66. "Watchful also discovered unpublished updates to TikTok and Douyin's terms of service that cover privacy and usage of the deepfakes feature. Inside the U.S. version of TikTok's Android app, English text in the code explains the feature and some of its terms of use: 'Your facial pattern will be used for this feature. Read the Drama Face Terms of Use and Privacy Policy for more details. Make sure you've read and agree to the Terms of Use and Privacy Policy before continuing. 1. To make this feature secure for everyone, real identity verification is required to make sure users themselves are using this feature with their own faces. For this reason, uploaded photos can't be used; 2. Your facial pattern will only be used to generate face-change videos that are only visible to you before you post it. To better protect your personal information, identity verification is required if you use this feature later. 3. This feature complies with Internet Personal Information Protection Regulations for Minors. Underage users won't be able to access this feature. 4. All video elements related to this feature provided by Douyin have acquired copyright authorization.'"[49]

67. Defendants also use their powerful biometrics engine to tailor user experiences in the TikTok App. Specifically, when a person's face or voice appears in a video uploaded to the TikTok App, Defendants' sophisticated technology creates a voiceprint derived from the unique

[48] Josh Constine, *ByteDance & TikTok have secretly built a deepfakes maker*, TechCrunch (Jan. 3, 2020), https://techcrunch.com/2020/01/03/tiktok-deepfakes-face-swap/.

[49] *Id.*

characteristics of the person's voice or a face template derived from the unique characteristics of the person's face, and then compares the generated voiceprint or face template against the voiceprints and face templates already stored in their database (which are already associated with the names and other personal information pertaining to the persons from whom this biometric data was collected). If there is a match, then Defendants are able to confirm the identity of the child appearing in the uploaded video – valuable information that Defendants use to further enhance the quality of the child's voiceprint or face template stored in its database and the functionality of the various features available on the TikTok App.

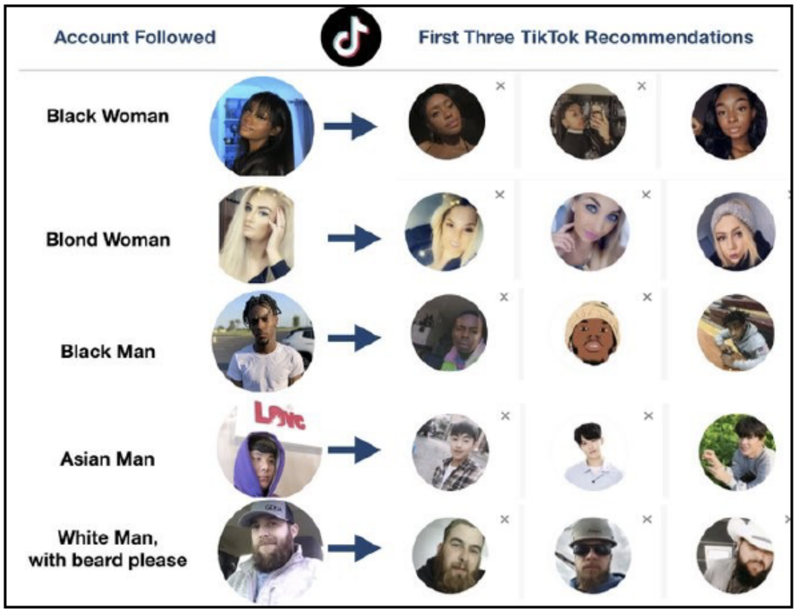
68. The flagship feature of the TikTok App is the "For You" recommendation engine. Prominently displayed to the user every time the TikTok App is loaded, the "For You" feature uses an algorithmic feed to recommend targeted videos for each user, even if the user never posted anything, followed anyone, or liked a video. The feature is powered by TikTok's AI algorithm, which continuously records each action users take on the App, including what videos each user watches, how long each user watches a particular category of video, and which advertisements a user engages with, as well their current location, and thus provides Defendants with "years of data informing it on how people think, feel and act, making it an expert on what makes people tick and how to persuade them to watch, share or like certain content."[50]

69. TikTok's AI algorithm is then able to use that information to tailor video recommendations to a particular user, including by referencing the immutable biometric data that Defendants have collected and stored for each person whose face or voice appears in a video viewed by the user on the TikTok App, along with the name, age, race, gender, and contact details of each such person that Defendants have derived from their biometric data.

70. Thus, in February 2020, Marc Faddoul, an AI researcher at UC Berkeley School of Information, found that TikTok was recommending accounts on users' "For You" page that

[50] Shelly Banjo, *Take China's TikTok App Security Threat Seriously*, Bloomberg (Oct. 29, 2019). https://www.bloomberg.com/news/newsletters/2019-10-29/worries-that-tiktok-is-a-threat-to-national-security-have-merit.

matched the race, age or facial characteristics of the user.[51] Mr. Faddoul found that when he followed the TikTok account of a black woman, the app recommended that he follow three more black women; that when he followed an Asian man with dyed hair, the app recommended three more Asian men with dyed hair; and that the same thing happened for men with visible disabilities. The following chart details some of Mr. Faddoul's findings:[52]


Account Followed
First Three TikTok Recommendations
Black Woman
Blond Woman
Black Man
Asian Man
White Man, with beard please

71. These features have been credited with having a "huge impact on user involvement and allowed TikTok to grow its audience organically."[53] TikTok's algorithm and features are so successful that the average person spends 45 minutes per day scrolling through the app.[54]

[51] Maria Mellor, *Why is TikTok creating filter bubbles based on your race*, Wired UK (Feb. 28, 2020), https://www.wired.co.uk/article/tiktok-filter-bubbles.

[52] *Marc Faddoul*, Twitter (Feb. 24, 2020), https://twitter.com/MarcFaddoul/status/1232014908536938498.

[53] Banuba, *How Camera Face Filters Brought TikTok Millions of Users*, Medium (Sept. 3, 2019), https://medium.com/@banuba/how-camera-face-filters-brought-tiktok-millions-of-users-4081f885f81c.

[54] Georgia Wells, Yang Jie, Yoko Kubota, *TikTok's Videos Are Goofy. Its Strategy to Dominate Social Media Is Serious*, Wall Street Journal (June 29, 2019), https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861.

72. The TikTok App's ability to extract and use voiceprints and face prints to identify people, and to recognize their age, race, and gender, is powered by technology developed and patented by Beijing ByteDance Technology Co Ltd, an affiliate of Defendants.[55]

73. ByteDance also licenses and otherwise provides access to its TikTok App APIs to various mobile-application developers, including APIs that enable the use of its facial and voice recognition technology.[56]

74. None of this is a secret. ByteDance has publicly admitted that its AI technology is trained to, among other things, engage in "facial recognition for the filters" and that it has "buil[t] intelligent machines that are capable of understanding and analyzing text, images and videos using natural language processing and computer vision technology."[57]

75. Recently, the U.S. National Security Advisor warned that the TikTok App "'is getting facial recognition' on millions of Americans as well as mapping their relationships, and then sending all of this 'intimate data' back to China for processing."[58]

76. And numerous media outlets have reported on Defendants' biometric data-collection efforts on the TikTok App, specifically in the facial and voice recognition contexts. For

[55] *See, e.g.,* "Voice recognition method for mobile terminal and device thereof," U.S. Patent No. US9502035B2, Beijing ByteDance Technology Co Ltd., Published April 7, 2016, *available at* https://patents.google.com/patent/US9502035B2; "Method and device for social platform-based data mining," U.S. Patent No. US10360230B2, Beijing ByteDance Technology Co Ltd., Published Nov. 9, 2017, *available at* https://patents.google.com/patent/US10360230B2.

[56] *See, e.g., Alexa for Apps*, Amazon, *available at* https://developer.amazon.com/en-US/alexa/alexa-skills-kit/get-deeper/response-api/alexa-for-apps (last accessed Sept. 8, 2020) ("TikTok created a first-of-its-kind experience for their platform with Alexa, offering voice-activated search and navigation in the app powered by Alexa. Mobile users can ask Alexa to search for videos, find music, and start a recording!")

[57] Sam Byford, *How China's Bytedance became the world's most valuable startup*, The Verge (Nov. 30, 2018), https://www.theverge.com/2018/11/30/18107732/bytedance-valuation-tiktok-china-startup.

[58] Zach Dorfman, *TikTok sale drama clouds the app's genuine security concerns*, Axios (Aug. 5, 2020), https://www.axios.com/tiktok-security-concerns-china-f761bcca-476d-487e-8261-bd770d570ac7.html.

instance, Bloomberg news noted that "TikTok's owner, Beijing-based ByteDance, is a hit app factory that has spent the last decade learning how to use artificial intelligence, machine learning, and facial recognition to figure out what people like and serve them endless streams of entertainment tailored to their interests and emotions. Its apps are used by billions of people, including 1.45 billion global downloads for TikTok alone. The company has years of data informing it on how people think, feel and act, making it an expert on what makes people tick and how to persuade them to watch, share or like certain content."[59]

77. Jesse Hirsh, of the Center for International Governance Innovation, noted that "[l]ike any social media platform, TikTok is an instrument for massive data collection. Given the advanced AI employed by the app, which includes facial recognition, object recognition, voice recognition and location-based services, TikTok should be regarded as an element of an emerging new era of pervasive espionage. As Western governments worry about surveillance via Huawei's telecommunications technology, should they also be concerned about surveillance through Chinese-owned social media?"[60]

78. ByteDance has also acknowledged that it collects biometric data in its TikTok clone apps around the globe. For example, the Vigo Video app, owned by TikTok Pte. Ltd, states in its Privacy Policy (Last Updated: January 1, 2020), that it "collect[s] and use[s]" a user's "face landmarks or face contour[.]"[61] Douyin's Privacy Policy similarly states that it uses "face recognition" to "perform real-name authentication."[62]

[59] Banjo, *supra* note 50.

[60] Jesse Hirsh, *New Platform, Old Problems: How TikTok Recreates the Regulatory Challenges that Came Before It*, Center for International Governance Innovation (May 18, 2020), https://www.cigionline.org/articles/new-platform-old-problems-how-tiktok-recreates-regulatory-challenges-came-it (last accessed Sept. 8, 2020)

[61] *Privacy Policy*, Vigo Video (Jan. 1, 2020), https://www.vigovideo.net/hotsoon/in_app/privacy_policy/.

[62] *"Tik Tok" Privacy Policy*, Douyin (Feb. 13, 2020), https://www.douyin.com/agreements/?id=6773901168964798477 (translation provided by Google Translate).

79. Notably, the Chinese government's recent export restrictions – spurred by President Trump's executive order effectively mandating that ByteDance divest TikTok to U.S. based company by September 20, 2020 in order for the company to continue operating in the United States –specifically restrict Chinese companies' ability to export the biometrics-collection and recognition technologies at issue in this case.[63]

80. Meanwhile, Defendants' efforts to improve their voice-recognition and facial-recognition capabilities remain ongoing.[64]

81. Publicly accessible job postings soliciting research scientists to join ByteDance and TikTok further confirm their continued innovations in the area of speech recognition.[65]

[63] *See* Eva Xiao, *TikTok Talks Could Face Hurdle as China Tightens Tech Export Rules*, Wall Street Journal (Aug. 30, 2020), https://www.wsj.com/articles/china-tightens-ai-export-restrictions-11598703527 (describing China's recent restrictions on exporting technologies, imposed specifically in response to the President Trump's executive order mandating a sale of TikTok's assets to a U.S.-based acquirer to continue operating in the U.S., as targeting "such computing and data-processing technologies as text analysis, content recommendation, speech modeling and voice-recognition")

[64] *See e.g.*, Mathieu Duchâtel and Théophile Lenoir, *Tiktok and Regulating Social Networks*, Institut Montaigne (June 9, 2020), https://www.institutmontaigne.org/en/blog/tiktok-and-regulating-social-networks ("TikTok is developing cutting-edge tools for facial, image and voice recognition, rivalling with the capabilities of American giants.").

[65] *See, e.g., Speech Recognition Scientist*, TikTok, *available at* https://careers.tiktok.com/position/detail/6837642029561874696 (last accessed Sept. 8, 2020) (soliciting applications for position in which employee will "[b]uild core technologies and carry out cutting-edge research in multilingual speech recognition field, e.g., acoustic and language models optimization under low source conditions," [d]esign and deploy different speech recognition engines for supporting multilingual speech and language processing," "[c]ollaborate with linguistic experts for building data collection and labeling pipeline," and "[e]xplore the next generation of speech understanding technology, and publish academic papers"); *Research Scientist in Speech & Audio*, LinkedIn, *available at* https://www.linkedin.com/jobs/view/1767638256 (last accessed Sept. 8, 2020) (soliciting applications for position at ByteDance in Mountain View, CA, in which employee will "[c]onduct cutting-edge research and development in speech & audio, multimodal processing (audio, vision and text), NLP and deep learning" and "[t]ransfer advanced technologies to ByteDance Products," and listing job requirements of, inter alia, experience in "speech recognition," "speaker recognition/diarization," "speech synthesis," "robust speech processing," "deep learning & representation learning, and "multimodal ML in audio, vision and text").

82. Thus, in less than two years, Defendants have collected, stored, used, and monetized the immutable and very "valuable" biometric data of hundreds of millions of its (mostly minor) users, millions of whom reside in Illinois, and without any of their consent – in clear violation of BIPA. And they are actively working to further finetune their abilities to collect and use this sensitive data in the future.

83. BIPA clearly prohibits what Defendants have done, and Defendants have made no effort to come into compliance with BIPA at any point in time (be it by obtaining the requisite signed written releases authorizing these practices or by turning the technology off in Illinois altogether).

IV. PLAINTIFF'S EXPERIENCES

84. At all times during the time period relevant to this action, Plaintiff has resided in Illinois and within this District. Using an account linked to his name and other personal details that he created on the TikTok App, and from within Illinois, Plaintiff has frequently logged into his account on the TikTok App using a mobile device and uploaded videos of himself that depicted his face and voice.

85. Upon uploading each such video, Defendants recorded, imaged, and analyzed Plaintiff's voice and face. Specifically, immediately after Plaintiff uploaded a video via the TikTok app depicting his face or voice, Defendants collected and analyzed a digital image of Plaintiff's face and a digital recording of his voice, which Defendants then used to extract, collect, store, and catalog Plaintiff's "voiceprint" and "face template" (i.e., a "scan of face geometry")—unique, immutable, and highly sensitive biometric identifiers used to identify a person—in their vast database of personally identifying biometric data.

86. Accordingly, Defendants collected Plaintiff's "biometric identifiers" as he used the TikTok App in Illinois. *See* 740 ILCS 14/10.

87. Defendants used the "voiceprint" and "scan of face geometry" that they extracted from Plaintiff's voice and face to, *inter alia*, identify him in other videos uploaded by him and other users on the TikTok App.

88. Specifically, each time Plaintiff's face or voice appeared in a video uploaded on the TikTok App, Defendants' sophisticated voice and/or facial recognition technology created a voiceprint of Plaintiff's voice and/or or a template of Plaintiff's face, and then compared the newly generated voiceprint or face template against the collection of voiceprints or face templates already stored in its database.

89. At that point, Defendants were able to match the newly collected voiceprint or face template with the voiceprints or face templates previously collected from the Plaintiff that were stored in their database and linked to the Plaintiff's identity. Defendants used this technology to confirm Plaintiff's identity in newly uploaded videos, improve the quality and detail of his voiceprints and face templates saved in their database, and better train the functionality of the various features available on their platform.

90. The unique voiceprints and face templates that Defendants extracted from Plaintiff's voice and face were not only collected and used by Defendants to identify Plaintiff by name, they allow Defendants to recognize Plaintiff's gender, age, race, and emotional states. Accordingly, Defendants collected Plaintiff's "biometric information" as he used the TikTok App in Illinois. *See* 740 ILCS 14/10.

91. In direct violation of §§ 15(b)(2) and 15(b)(3) of BIPA, Defendants never informed Plaintiff or his father, or the members of the Illinois Voice Subclass and Illinois Face Subclass or their parents, of the specific purpose and length of term for which their (or their children's) biometric identifiers and information would be collected, stored, and used, nor did Defendants ever ask for much less obtain a written release from any of these persons (or their parents in the case of children).

92. Neither Plaintiff M.G.'s father nor any other Illinois Voice Subclass or Illinois Face Subclass member's parent, legal guardian, or authorized representative received a disclosure from Defendants stating that they would collect, capture, otherwise obtain, or store unique biometric identifiers or biometric information extracted from their child's face or voice. Neither Plaintiff M.G.'s father, nor any other Illinois Voice Subclass or Illinois Face Subclass member's parent,

legal guardian, or authorized representative ever consented, agreed or gave permission—via a written release or otherwise—to authorize or permit Defendants to collect, capture, otherwise obtain, or store their child's sensitive biometric data or in this way.

93. Likewise, Defendants never provided Plaintiff M.G.'s father or any other parent, legal guardian, or authorized representative of any member of the Classes with an opportunity to prohibit or prevent the collection, storage, or use of their child's unique biometric identifiers, biometric information, or other personally identifying information.

94. In fact, Plaintiff, as a minor, was legally incapable of providing the "written release" required by BIPA to authorize Defendants' collection, storage, or use of his biometrics.

95. Moreover, in direct violation of § 15(a) of BIPA, Defendants do not have written, publicly available policies identifying their retention schedules, or guidelines for permanently destroying the biometric identifiers and biometric information it has collected from persons in Illinois.

96. Nevertheless, whenever a video was uploaded on the TikTok App from within Illinois that depicted the voice or face of Plaintiff or any other member of the Class, Defendants' sophisticated face and voice recognition technologies scanned the recording of the voice and the geometry of the face appearing in the video and created and stored a unique "voiceprint" and "face template" corresponding to the person, all in direct violation of BIPA.

V. BYTEDANCE IS ON THE VERGE OF DIVESTING ALL OF TIKTOK'S ASSETS TO A THIRD PARTY, AND TRANSFERRING THE BIOMETRIC DATA IT HAS AMASSSED TO THE ACQUIRING THIRD PARTY

97. Plaintiff and the other Illinoisans who have had their biometric data surreptitiously collected and stored by Defendants are entitled by law to have this sensitive data permanently destroyed. Further dissemination of this immutable biometric data would deny BIPA's promise of privacy precisely where it is needed the most.

98. Nonetheless, in light of the President's executive orders compelling ByteDance to divest TikTok to a domestic entity no later than September 20, 2020, and to divest itself of

TikTok's American user data by November 12, 2020, a transmission of their biometric data from Defendants to the Acquiring Entity is imminent.

99. TikTok maintains that it will transfer its users' data (which would include the BIPA-protected biometric data at issue in this action) to any entity that acquires the company.[66]

100. Thus, in light of the executive orders and TikTok's operative privacy policy, ByteDance's divestment to the Acquiring Entity of all of TikTok's assets and all of the TikTok App's users' data, including all of the "biometric identifiers" and "biometric information" collected by Defendants to date, is imminent and will occur no later than September 20, 2020.

101. Plaintiff and the members of the Illinois Subclasses have not consented, authorized, or provided "signed written releases" authorizing Defendants to transfer their "biometric identifiers" or "biometric information" to the Acquiring Entity.

102. Plaintiff and the members of the Illinois Subclasses have not consented, authorized, or provided "signed written releases" authorizing the Acquiring Entity to obtain their "biometric identifiers" or "biometric information" from Defendants.

103. Defendants' transfer the biometrics of Plaintiff and the Illinois Voice Subclass and Illinois Face Subclass members to the Acquiring Entity (or to any intermediary entity), absent the requisite signed written releases from Plaintiff and Illinois Voice Subclass and Illinois Face Subclass members, would be in clear violation of BIPA, 740 ILCS 14/15(d).

104. The Acquiring Entity's obtainment of the biometrics of Plaintiff and the Illinois Voice Subclass and Illinois Face Subclass members from Defendants, absent the requisite signed written releases from Plaintiff and the Illinois Voice Subclass and Illinois Face Subclass members, would also be in clear violation of BIPA, 740 ILCS 14/15(b)(3).

[66] *See Privacy Policy*, *supra* note 25 (under hearing "Sale or Merger," stating: "We disclose your information to third parties: in the event that we sell or buy any business or assets (for example, as a result of liquidation, bankruptcy or otherwise). In such transactions, we will disclose your data to the prospective seller or buyer of such business or assets; or if we sell, buy, merge, are acquired by, or partner with other companies or businesses, or sell some or all of our assets. In such transactions, user information may be among the transferred assets.").

105. Plaintiff and members of the Illinois Voice Subclass and Illinois Face Subclass would be irreparably harmed by Defendants' transfer of their "biometric identifiers" or "biometric information" to the Acquiring Entity, as such a transfer would further violate their statutorily right to privacy in their biometrics, would cause them to lose further control over this sensitive, immutable data, and put them at increased risk of identity theft, financial crimes, and other similar evils resulting from the continued proliferation of their biological data capable of identifying them.

106. Thus, Plaintiff seeks an Order enjoining Defendants from transferring Plaintiff's and the other Illinois Voice Subclass and Illinois Face Subclass members' biometrics to the Acquiring Party (or to any intermediary entity) in further violation of BIPA, and (2) compelling Defendants to destroy the biometrics of Plaintiff and the Illinois Voice Subclass and Illinois Face Subclass that they have collected and stored without consent.

CLASS ALLEGATIONS

107. **Class Definition**: Plaintiff, by and through his father and legal guardian, brings this action pursuant to Fed. R. Civ. P. 23 on behalf of two classes and subclasses of similarly situated individuals defined as follows (collectively, the "Classes"):

> **Voice Class:** All persons in the United States who had a recording of their voice collected by TikTok Inc. or ByteDance, Inc.
>
> **Face Class:** All persons in the United States who had an image of their face collected by TikTok Inc. or ByteDance, Inc.
>
> **Illinois Voice Subclass:** All persons who had a recording of their voice collected by TikTok Inc. or ByteDance, Inc. while residing in Illinois.
>
> **Illinois Face Subclass:** All persons who had an image of their face collected by TikTok Inc. or ByteDance, Inc. while residing in Illinois.

The following are excluded from the Classes: (1) any Judge presiding over this action and members of his or her family; (2) Defendants, each Defendant's subsidiaries, parents, successors, predecessors, and any entity in which any Defendant or its parent has a controlling interest (including current and former employees, officers, or directors); (3) persons who properly execute and file a timely request for exclusion from the Classes; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendants' counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

108. **Numerosity**: Pursuant to Fed. R. Civ. P. 23(a)(i), the number of persons within the Classes is substantial, believed to amount to millions of persons. It is, therefore, impractical to join all members of the Classes as named plaintiffs. Further, the size and relatively modest value of the claims of the individual members of the Classes renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation.

109. **Commonality, Typicality, and Predominance**: Pursuant to Fed. R. Civ. P. 23(a)(ii), (a)(iii), and (b)(3), there are well-defined common questions of fact and law that exist as to all members of the Classes, that are typical of Plaintiff's claims, and that predominate over any questions affecting only individual members of the Classes. These common legal and factual questions, which do not vary from member to member, and which may be determined without reference to the individual circumstances of any individual member, include but are not limited to the following:

a. whether Defendants collected, captured, or otherwise obtained "biometric identifiers" or "biometric information" from Plaintiff and the other members of the Classes in connection with their use of the TikTok App during the applicable statutory period(s);

b. whether Defendants stored Plaintiff's and the Classes' "biometric identifiers" or "biometric information";

c. whether Defendants informed Plaintiff and the Classes that it would collect, capture, otherwise obtain and then store their "biometric identifiers" or "biometric information";

d. whether Defendants obtained a written release (as defined in 740 ILCS 14/10) prior to collecting, capturing, or otherwise obtaining, and then storing, Plaintiff's and the Illinois Voice Class and Illinois Face Class members' "biometric identifiers" or "biometric information";

e. whether Defendants developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying the "biometric identifiers" and "biometric information" that it collected, captured, and otherwise obtained in Illinois when the initial purpose for collecting, capturing, or otherwise obtaining these "biometric identifiers" and "biometric information" has been satisfied or within 3 years of their last interaction with Plaintiff and members of the Illinois Voice Class and Illinois Face Class, whichever occurs first;

f. whether Defendants used Plaintiff's and the Classes' "biometric information" to identify them;

g. Whether Defendants' collection, capture, and obtainment of Plaintiff's and the Illinois Voice Class and Illinois Face Class members' "biometric identifiers" or "biometric information" violated BIPA from within Illinois;

h. whether Defendants' violations of BIPA were committed negligently;

i. whether Defendants' violations of BIPA were committed intentionally or recklessly;

j. whether Defendants were unjustly enriched by their nonconsensual collection of Plaintiff's and the Classes' biometrics;

k. Whether Defendants' transfer or dissemination of the biometrics of Plaintiff and the members of the Illinois Voice Class and Illinois Face Class to the Acquiring Entity would constitute a violation of BIPA;

l. Whether Defendants' transfer or dissemination of the biometrics of Plaintiff and the members of the Classes to the Acquiring Entity would constitute unjust enrichment;

m. Whether Plaintiff has demonstrated a substantial likelihood that Defendants will transfer the biometrics of Plaintiff and the members of the Illinois Voice Class and Illinois Face Class to the Acquiring Entity (or to any intermediary entity) in connection with the Acquiring Entity's acquisition of TikTok; and

n. Whether Defendants should be enjoined from transferring the biometrics of Plaintiff and the members of the Illinois Voice Class and Illinois Face Class to the Acquiring Entity.

110. **Adequate Representation**: Pursuant to Fed. R. Civ. P. 23(a)(iv), Plaintiff has retained and is represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation. Plaintiff and his counsel are committed to vigorously prosecuting this class action. Neither the Plaintiff nor any of his counsel have any interest adverse

to, or in conflict with, the interests of the absent members of the Classes. Plaintiff is able to fairly and adequately represent and protect the interests of the Classes. Plaintiff has raised viable statutory claims of the type reasonably expected to be raised by members of the Class, and will vigorously pursue those claims. If necessary, Plaintiff may seek leave of court to amend this Complaint to include additional representatives to represent the Classes or to add additional claims or classes, as appropriate.

111. **Superiority**: Pursuant to Fed. R. Civ. P. 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all members of the Classes is impracticable. Even if every member of the Classes could afford to pursue individual litigation, the Court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent or contradictory judgments, and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system and protects the rights of each member of the Class. Plaintiff anticipates no difficulty in the management of this action as a class action. Class-wide relief is essential to compel compliance with BIPA.

FIRST CAUSE OF ACTION
Violation of 740 ILCS 14/15.
(On Behalf of Plaintiff and the Illinois Voice Subclass and Illinois Face Subclass)

112. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

113. BIPA makes it unlawful for any private entity to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the

subject of the biometric identifier or biometric information or the subject's legally authorized representative." 740 ILCS 14/15(b).

114. Plaintiff's father and legal guardian, Bartosz Grabowski, is Plaintiff's "legally authorized representative" within the meaning of BIPA and served in such capacity at all times relevant to this action. See 740 ILCS 14/15 (b).

115. Defendants are corporations and thus each qualify as a "private entity" under the BIPA. See 740 ILCS 14/10.

116. Whenever a video depicting Plaintiff's or an Illinois Voice Subclass and Illinois Face Subclass member's face or voice was uploaded via the TikTok App, Defendants recorded, imaged, and analyzed the depicted voice and face. Specifically, immediately after Plaintiff or an Illinois Voice Subclass and Illinois Face Subclass member uploaded a video via the TikTok app depicting their face or voice, Defendants collected and analyzed a digital image of the face and a digital recording of the voice, which Defendants then used to extract, collect, store, and catalog Plaintiff's and each Illinois Voice Subclass and Illinois Face Subclass member's "voiceprint" and "face template" (i.e., a "scan of face geometry")—unique, immutable, and highly sensitive biometric identifiers used to identify a person—in their vast database of personally identifying biometric data.

117. Thus, Plaintiff and the members of the Illinois Voice Subclass and Illinois Face Subclass are persons who had their "biometric identifiers," including their voiceprints and scans of face geometry, collected, captured, received, or otherwise obtained by Defendants in connection with their use of the TikTok App in Illinois within the preceding five (5) years. *See* 740 ILCS 14/10.

118. Plaintiff and all members of the Illinois Voice Subclass and Illinois Face Subclass are also persons who had their "biometric information" collected by Defendants (in the form of their gender, age, race, and emotional state) through Defendants' collection and use of personally identifying information derived from their "biometric identifiers" that Defendants have used to identify them.

119. Defendants systematically collected, captured, or otherwise obtained Plaintiff's and the Illinois Voice Subclass and Illinois Face Subclass members' "biometric identifiers" and "biometric information" without first obtaining signed written releases, as required by 740 ILCS 14/15(b)(3), from any of them or their "legally authorized representatives," *i.e.*, their parents or legal guardians.

120. In fact, Defendants failed to properly inform Plaintiff or members of the Illinois Voice Subclass or Illinois Face Subclass, or any of the foregoing's parents, legal guardians, or other "legally authorized representatives," in writing that Plaintiff's or the Illinois Voice Subclass and Illinois Face Subclass members' "biometric identifiers" and "biometric information" were being "collected or stored" by Defendants, nor did Defendants inform Plaintiff or members of the Illinois Voice Subclass or Illinois Face Subclass, or any of the foregoing's parents, legal guardians, or other "legally authorized representatives," in writing of the specific purpose and length of term for which their "biometric identifiers" and "biometric information" were being "collected, stored and used" as required by 740 ILCS 14/15(b)(1)–(2).

121. In addition, Defendants do not publicly provide a retention schedule or guidelines for permanently destroying the "biometric identifiers" and "biometric information" of Plaintiff or the members of the Illinois Voice Subclass or Illinois Face Subclass, as required by the BIPA. *See* 740 ILCS 14/15(a).

122. Defendants have denied BIPA's promise of privacy to those who need it most. By collecting, storing, and using Plaintiff's and the other Illinois Voice Subclass and Illinois Face Subclass members' "biometric identifiers" and "biometric information" as described herein, Defendants recklessly or intentionally violated each of BIPA's requirements, and infringed Plaintiff's and the other Illinois Voice Subclass and Illinois Face Subclass members' rights to keep their sensitive, immutable, and uniquely identifying biometric data private.

123. Plaintiff is informed and believes that ByteDance's divestment to the Acquiring Entity (or an intermediary entity) of all of TikTok's assets and all of the TikTok App's users' data,

including all of the "biometric identifiers" and "biometric information" collected by Defendants to date, is imminent and will occur by September 20, 2020.

124. Plaintiff and the Illinois Voice Subclass and Illinois Face Subclass members have not consented, authorized, or provided "signed written releases" authorizing Defendants to transfer their "biometric identifiers" or "biometric information" to the Acquiring Entity (or to any intermediary entity).

125. Defendants' transfer the biometrics of Plaintiff and the Illinois Voice Subclass and Illinois Face Subclass members to the Acquiring Entity (or to any intermediary entity), absent the requisite signed written releases from the Plaintiff and Illinois Voice Subclass and Illinois Face Subclass members, would be in clear violation of BIPA, 740 ILCS 14/15(b)(3).

126. Plaintiff and members of the Illinois Voice Subclass and Illinois Face Subclass would be irreparably harmed by Defendants' transfer of their "biometric identifiers" or "biometric information" to the Acquiring Entity (or to any intermediary entity), as such a transfer would further violate their statutory right to privacy in their biometrics, would cause them to lose further control over this sensitive, immutable data, and put them at increased risk of identity theft, financial crimes, and other similar evils resulting from the continued proliferation of their biological data capable of identifying them.

127. Plaintiff seeks a Court order requiring Defendants to destroy Plaintiff's and the Illinois Voice Subclass and Illinois Face Subclass members' biometrics, and temporarily and permanently enjoining Defendants from transferring Plaintiff's and the Illinois Voice Subclass and Illinois Face Subclass members' biometrics to the Acquiring Entity in further violation of BIPA

128. On behalf of himself and the members of the Illinois Voice Subclass and Illinois Face Subclass, by and through his father and natural legal guardian, Bartosz Grabowski, Plaintiff seeks: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the other members of the Illinois Voice Subclass and Illinois Face Subclass by requiring Defendants permanently destroy the biometric data they have collected from persons in Illinois to date and to refrain from collecting or transferring such data in the future, to the Acquiring Entity, any

intermediary entity, or otherwise, absent the requisite prior informed written authorization of their legally authorized representatives; (2) statutory damages of $1,000.00 to Plaintiff and each Illinois Voice Subclass and Illinois Face Subclass member pursuant to 740 ILCS 14/20 for each negligent violation of BIPA committed by Defendants; (3) statutory damages of $5,000.00 to Plaintiff and each Illinois Voice Subclass and Illinois Face Subclass member pursuant to 740 ILCS 14/20 for each intentional or reckless violation of BIPA committed by Defendants; and (4) reasonable attorneys' fees and costs and other litigation expenses to Plaintiff's counsel and proposed counsel for the Illinois Voice Subclass and Illinois Face Subclass pursuant to 740 ILCS 14/20(3).

SECOND CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Classes)

129. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

130. Plaintiff and the members of the Classes conferred a benefit on Defendants by downloading and using the TikTok App. Specifically, Plaintiff and the Classes provided valuable data to Defendants—including contact data, personal demographic information, usage data, and biometrics—that TikTok was able to use to improve its services, increase sales and advertising revenue, and, most importantly, to improve its AI algorithms.

131. Defendants knowingly and willfully accepted and enjoyed those benefits. Indeed, Defendants' entire business model depends on siphoning user data to train their AI platforms.

132. Defendants knew or should have known that the benefits provided by Plaintiff and the Classes—sensitive personal data—were not given freely and willfully, as Defendants chose not to fully disclose their biometric collection practices (despite doing so elsewhere in the world).

133. By willfully collecting sensitive user data without consent from Plaintiff or the Classes, Defendants gained materially valuable data, which in turn led to windfall profits.

134. To allow Defendants to profit from their brazen spy tactics would be unjust and inequitable. Principles of equity demand disgorgement of the TikTok Defendant's ill-gotten gains to Plaintiff and the Classes.

135. On behalf of himself and the proposed members of the Classes, by and through his father and natural legal guardian, Bartosz Grabowski, Plaintiff seeks: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the other members of the Classes; and (2) restitution in the form of disgorgement of all profits, benefits, and other compensation obtained by Defendants through their unjust conduct.

PRAYER FOR RELIEF

WHEREFORE, on behalf of himself and all others similarly situated, Plaintiff M.G., a minor, by and through his father and legal guardian, Bartosz Grabowski, seeks judgment against Defendants as follows:

A. Certifying this case as a class action on behalf of the Classes defined above, appointing Plaintiff, by and through his father and legally authorized guardian, Bartosz Grabowski, as representative of the Classes, and appointing his counsel as Class Counsel on behalf of the Classes;

B. Declaring that Defendants' actions, as set out above, violate the BIPA, 740 ILCS 14/1, *et seq.,* with respect to Plaintiff and members of the Illinois Voice Subclass and Illinois Face Subclass;

C. Awarding $1,000.00 statutory damages to Plaintiff and each member of the Illinois Voice Subclass and Illinois Face Subclass pursuant to 740 ILCS 14/20(1) for each violation of BIPA committed by Defendants negligently, or $5,000.00 pursuant to 740 ILCS 14/20(2) for each violation of BIPA committed by Defendants intentionally or recklessly;

D. Awarding restitution to Plaintiff and the Classes in the form of disgorgement of all profits, benefits, and other compensation obtained by Defendants through their unjust conduct.

E. Awarding injunctive and other equitable relief pursuant to BIPA as is necessary to protect the interests of Plaintiff and members of the Illinois Voice Subclass and Illinois Face Subclass, including, *inter alia*, an order requiring Defendants to collect, store, use, refrain from transferring (to the Acquiring Entity or otherwise) the biometric identifiers and biometric information of Plaintiff and members of the Illinois Voice Subclass and Illinois Face Subclass in compliance with BIPA, and to permanently destroy the biometric identifiers and biometric information they have collected from Plaintiff and the Illinois Voice Subclass and Illinois Face Subclass members to date;

F. Awarding Plaintiff's counsel and proposed counsel for the Classes their reasonable litigation expenses and attorneys' fees;

G. Awarding Plaintiff and the Classes pre- and post-judgment interest, to the extent allowable;

H. Awarding Plaintiff and the Classes such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff demands a trial by jury on all claims and issues so triable.

Dated: September 8, 2020

Respectfully submitted,

s/ J. Dominick Larry

NICK LARRY LAW LLC
J. Dominick Larry
55 E Monroe St, Suite 3800
Chicago, IL 60603
Tel: (773) 694-4669
Fax: (773) 694-4691
Email: nick@nicklarry.law

Local Counsel for Plaintiff, by and through his father and legal guardian Bartosz Grabowski, and the Putative Classes

HEDIN HALL LLP
Frank S. Hedin*
David W. Hall*
1395 Brickell Avenue, Suite 1140
Miami, Florida 33131
Tel: (305) 357-2107
Fax: (305) 200-8801
E-mail: fhedin@hedinhall.com
dhall@hedinhall.com

BURSOR & FISHER, P.A.
Scott A. Bursor *
Joseph I. Marchese*
Joshua D. Arisohn*
Philip L. Fraietta*

888 Seventh Avenue
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
E-Mail: scott@bursor.com
jmarchese@bursor.com
jarisohn@bursor.com
pfraietta@bursor.com

**Pro Hac Vice Application Forthcoming*

Counsel for Plaintiff, by and through his father and legal guardian Bartosz Grabowski, and the Putative Classes